Richmond Journal of Law and Technology

Volume 5 | Issue 2 Article 6

1998

How Have Internet Service Providers Beat Spammers?

Cathryn Le
University of Richmond

Volume V, Issue 2, Winter 1998

How Have Internet Service Providers Beat Spammers?

Cathryn Le[*]

Cite As: Cathryn Le, Note, How Have Internet Service Providers Beat Spammers?, 5 RICH. J.L. & TECH. 9, (Winter 1998) <http://www.richmond.edu/jolt/v5i2/le.html>.[**]

I. Introduction

{1} Popularly known as cyberspace, the Internet continues to evolve and expand, keeping pace with the lives of its users as a complex communications network. Many people rely on the Internet, an intricate link of numerous computers and computer networks, as a research and communications tool. The Internet is a "decentralized, global medium of communications--or 'cyberspace'--that links people, institutions, corporations, and governments around the world."[1] No single entity owns the Internet, but the individual computers that compose the Internet are owned by various individuals, governmental, public and private organizations and institutions.[2] The Internet cannot have a main control center nor can any single entity

monopolize the abundant variety of information freely accessible on the Internet;[3] however, the finite computer networks that comprise the Internet are intertwined in a manner which permits a computer linked to the Internet to interact with other computers linked to the Internet. This interconnection among computers and computer networks is the means by which the rapid exchange of electronic information can occur.[4]

{2} People who seek access to the Internet may obtain membership from a number of Internet service providers ("ISPs") such as America Online, CompuServe, Prodigy, and other local ISPs. These Internet service providers offer membership based on a flat monthly or yearly fee or on an hourly rate. In recent years, most, if not all, members choose to pay the flat monthly or yearly rate in light of their extensive use of the Internet.[5] After an individual purchases access from an ISP, that individual may use the Internet to communicate with another individual who has Internet access via electronic mail, more commonly known as "e-mail". E-mail communication "occur[s] almost instantaneously, and can be directed either to specific individuals, to a broader group of people interested in a particular subject, or to the world as a whole."[6] Users of the Internet range from government officials to children.

{3} As a new method of communication develops, it undeniably creates an additional channel through which unsolicited commercial advertisements can be sent. E-mail has provided businesses with an attractive avenue with which to advertise their products and services.[7] These advertisements, referred to as "junk e-mail" or "spam,"[8] have enraged many who communicate via e-mail. Spam is "increasing at an exponential rate."[9] Businesses incur minimal cost through mass e-mail advertisements because Internet users are not charged for the amount of information they send.[10] Bulk e-mailing takes only minutes to complete, and the advertisements are transmitted to the recipients' electronic mail boxes almost instantaneously, regardless of geographical location. This method of advertising is faster and cheaper than any other means of cold advertising, including door-to-door, phone, and postal mail solicitations. For those reasons, many businesses have an interest in protecting their alleged right to send unsolicited e-mail advertisements to Internet users. Their persistence is evident in several cases that have been filed by Internet service providers against spammers.[11]

{4} Unsolicited e-mail advertisements[12] may be annoying to some Internet users but whether this practice can be legally restricted or regulated has yet to be determined. This discussion may trigger free speech concerns. Many spammers assert freedom of speech as a defense. Notwithstanding the free speech defense, many Internet service providers have been successful in their fight against spammers. Part II of this paper discusses the standard of judicial scrutiny that the courts have applied in free speech cases and assesses whether a restriction of unsolicited advertisements via e-mail encroaches upon this fundamental right. Part III examines two other possible defenses that spammers may employ to protect their challenged right to send unsolicited e-mail. Part IV analyzes cases and complaints seeking redress against unsolicited e-mail advertisements. Part V evaluates both state and federal legislative developments that have occurred in response to spam-related litigation. Part VI presents the legal theories which have been most successful in obtaining judgments against spammers, in light of the judicial and legislative developments presented in Parts IV and V. Part VII proposes a recommendation for the future development of the law governing unsolicited e-mail advertisements. Finally, Part VIII concludes with a prediction of the direction in which the law is developing.

II. Judicial Scrutiny Applicable To Free Speech Cases

A. "*Commercial Speech*" *Is Not an Exception To the First Amendment*

{5} Freedom of speech traditionally has been viewed "to assure unfettered interchange of ideas for the bringing about of *political* and *social* changes desired by the people."[13] In 1942, when the United States Supreme Court first confronted a restriction of purely commercial speech, the Court asserted that "[w]e are . .

. clear that the Constitution imposes no . . . restraint on government as respects purely commercial advertising."[14] After 1951, the Court veered away from denying protection under the First Amendment[15] when the nature of the speech was purely commercial.[16] In 1976, however, the Supreme Court explicitly declared that "commercial speech, like other varieties of speech, is protected"[17] under the First Amendment of United States Constitution.

B. *The Central Hudson/Fox Standard of Scrutiny*

{6} Although the United States Supreme Court acknowledges that commercial speech is a freedom guaranteed by the United States Constitution, the Court grants less protection to commercial speech than non-commercial speech.[18] In 1980, the Court established an intermediate level of scrutiny in reviewing government regulations that restrict commercial speech.[19] *Central Hudson Gas & Electric Corp. v. Public Service Commission*[20] developed a four-pronged test to determine whether commercial speech has been unconstitutionally restricted. Governmental regulation of commercial speech is valid if the following factors are present: (1) the speech concerns an unlawful activity and is misleading; (2) the asserted governmental interest is substantial; (3) the regulation directly advances the governmental interest asserted; and (4) the regulation is narrowly tailored to serve that interest.[21] Not all of the factors, however, are needed for the regulation to be valid.[22] In complying with the requirements of intermediate scrutiny, the government has to show that spamming causes actual harm and that the government regulation "will in fact alleviate the real harm to a material degree."[23] The government regulation, however, does not have "to be the least restrictive means available; rather, there [only needs to] be a 'reasonable fit' between the government interest and the regulation."[24]

C. *The Intermediate Standard as Applied to Mail, Door-to-Door, Phone, and Fax Solicitations*

{7} In determining whether to restrict unsolicited communications, courts have sought to balance the right to freedom of speech with an individual's right to privacy. The United States Supreme Court has been hesitant to allow governmental regulation of advertisements sent through the U.S. mail. The only regulation that has withstood judicial scrutiny is one in which the government granted recipients the choice of blocking unsolicited mail advertisements.[25] Door-to-door solicitations face a more stringent regulation because of their greater encroachment on the recipient's privacy; therefore, statutes may require that the solicitation occur at a reasonable time, place, and manner.[26] Phone solicitations have been subject to the most government interference. Not only does the law require telemarketers to identify themselves, to allow recipients to decline the communication, and to restrict calls to reasonable times,[27] but federal regulations prohibit artificial or prerecorded telephone solicitations.[28]

{8} The most striking ban on commercial speech to pass judicial muster targets unsolicited advertisements via facsimile machines. Section 227(b)(1)(C) of the Telephone Consumer Protection Act of 1991 ("TCPA") explicitly states that no "telephone facsimile machine, computer, or other device [can be used] to send an unsolicited advertisement to a telephone facsimile machine."[29] In *Destination Ventures, Ltd. v. Federal Communications Commission*,[30] several businesses that wanted to advertise via facsimile machine and several businessmen who wanted to continue receiving fax solicitations challenged the constitutionality of this provision of the TCPA. Those plaintiffs requested that the court enjoin the enforcement of this section of the TCPA based on their contention that the section violated their freedom of speech. Applying the intermediate level of scrutiny, the court upheld the constitutionality of the TCPA.[31]

D. *The Intermediate Standard as Applied to Electronic Mail*

1. Spamming and the Telephone Consumer Protection Act

{9} One proposed theory for eliminating spam from the Internet is to include it in the stark prohibition

against fax solicitation, provided for in section 227(b)(1)(C) of the TCPA and upheld in *Destination Ventures, Ltd. v. Federal Communications Commission*, discussed above. This argument is not sound. In *Destination Ventures*, the court found that section 277(b)(1)(C) of the TCPA directly advanced (and was narrowly tailored to fit) the government's substantial interest in preventing the cost of advertising from being unfairly shifted from the sender to the recipient; it also prevents desired business messages from being impeded.[32] This raises the question of whether these two government interests apply when a person sends unsolicited commercial advertisements via e-mail.

{10} To fully examine the possible application of the TCPA to unsolicited e-mails, an assumption must be made that the TCPA encompasses such advertisements. Even if that assumption is made, the government must jump over the constitutional hurdle and show that the government interests expressed in *Destination Ventures* also apply to unsolicited e-mails before the government is able to impose such a strict regulation. The argument that spammers are shifting the cost of advertising to recipients is strengthened if ISP subscribers are charged in hourly increments for Internet access. In such a case, there is an element of cost-shifting because subscribers have to pay for the time that it takes them to shuffle through, read, and delete "junk e-mail."

{11} Although most commercial online computer services permit their subscribers to pay incrementally, the overwhelming majority choose to pay a more competitive monthly rate for Internet access.[33] As such, recipients "incur no marginal cost . . . for the time it takes them to throw out the spam."[34] Even if the government could successfully argue that the cost of advertising is being shifted to ISPs (because the receipt of mass electronic mail messages burdens the servers[35] and drains the resources of Internet service providers),[36] the question remains whether those ISPs are "recipients" of the advertisement as the term is used in *Destination Ventures, Ltd.* The court in *Destination Ventures* upheld the constitutionality of a complete ban on soliciting via facsimile, in part, because the cost of such advertising is shifted to the "unwitting customer."[37] An argument could be made that the recipients of the advertisement are the potential consumers (the subscribers of the ISPs), not the ISPs themselves.

{12} In addition, although a facsimile machine cannot process another message while it is printing an incoming one, a computer has the capability to process and store numerous e-mail messages simultaneously. Internet service providers contend that the large volume of "junk e-mail" occupies a substantial amount of disk space and exhausts the processing power of their computer equipment.[38] This may place a burden on an ISP's equipment and delay the delivery of e-mails, but the problem has not reached the magnitude of "thwart[ing] the receipt of legitimate and important messages."[39] Local ISPs, however, could have smaller storing capacity and the burden of storing and processing spam could hamper the computer system's ability to store and process other e-mail. If the volume of mass e-mail explodes, it potentially could reach a point where legitimate messages might be thwarted because no ISP has infinite storing capacity. Based on present allegations, however, a solid argument cannot be made that either of the harms used to justify the enactment of section 277(b)(1)(C) of the TCPA are present with respect to unsolicited e-mails. Interpretation of this statute to include electronic mail may, therefore, be an unconstitutional infringement of freedom of speech.

{13} As stated previously, the above discussion is based on the assumption that the government has imposed a restriction on unsolicited e-mail advertisements. Congress, however, has never indicated the intent to expand the federal prohibitions of the TCPA to include electronic mail. The actual text of the statute targets unsolicited advertisements via the telephone system, but extending the prohibition to include e-mails would exceed the original meaning and intent of the TCPA. Congress could have used the phrase "electronic communications," which it has used in previous federal statutes, in place of the chosen phrase "telephone facsimile machine"[40] to include both fax machines and computer transmitted e-mails. The failure of Congress to do so indicates that "Congress had a very specific type of nuisance in mind."[41] Congress made a further distinction between a computer and a fax machine by prohibiting the use of a computer to send advertisements to a telephone facsimile machine.[42] Accordingly, the argument in favor of the inclusion of

electronic mail under the fax prohibition lacks support.

2. Cyber Promotions, Inc. v. America Online, Inc.[43]

{14} Spammers like Sanford Wallace, also known as the "Spam King" and president of Cyber Promotions, Inc. ("Cyber Promotions"),[44] defend their actions by asserting their right to freedom of speech.[45] That defense, however, has been rejected by two different courts. The United States District Court for the Eastern District of Pennsylvania rejected a freedom of speech defense in *Cyber Promotions, Inc. v. America Online, Inc.*[46] Cyber Promotions had been sending unsolicited commercial advertisements via e-mail to America Online, Inc. ("AOL") subscribers, who made numerous complaints with regard to Cyber Promotions' actions.[47] As a result, AOL informed Cyber Promotions that it wanted the solicitations to cease.[48] When the e-mail persisted, AOL filtered and collected all of the unsolicited e-mail and returned them in bulk to Cyber Promotions' ISP.[49] Cyber Promotions filed a complaint in response to AOL's actions, requesting that the court grant it the right to continue sending unsolicited e-mail advertisements and to enjoin AOL from blocking the receipt of such e-mail messages.[50] The court, finding that AOL was not a state actor nor a public utility, held that Cyber Promotions' actions did not invoke the protection of the First Amendment and granted AOL a partial summary judgment on this issue.[51]

3. CompuServe Inc. v. Cyber Promotions, Inc.

{15} After the district court's decision in 1996, Cyber Promotions moved on to the next ISP. CompuServe Inc.. ("CompuServe") in *CompuServe, Inc. v. Cyber Promotions, Inc.*,[52] found itself in a similar position to AOL. Many of CompuServe's subscribers, who pay incrementally for their service, wanted to terminate their enrollment and to purchase access from another ISP to avoid the annoyance of unsolicited e-mails.[53] CompuServe subsequently prohibited Cyber Promotions from sending any further mailings of unsolicited advertisements to CompuServe subscribers. Cyber Promotions, however, ignored CompuServe's request. CompuServe then installed a filtration software to screen out all unsolicited e-mails. Nonetheless, Cyber Promotions was able to alter its spams to evade the screening software installed by CompuServe.

{16} As a result, CompuServe sought to have Cyber Promotions's advertising methods declared a trespass to chattels. Cyber Promotions again claimed protection under freedom of speech. The United States District Court for the Southern District of Ohio, however, rejected Cyber Promotions' free speech argument and granted CompuServe a preliminary injunction.[54]

4. First Amendment Defense

{17} Generally, spammers have defended their actions by asserting their right to freedom of speech. To invoke the protection of the First Amendment, however, a business's freedom of speech has to be restricted by a governmental entity.[55] Internet service providers such as AOL and CompuServe are not state actors;[56] they are private companies. As such, these ISPs have the right to restrict access to their property by use of any legal means available. For example, Internet service providers may employ blocking[57] or filtration[58] devices to prevent their members from receiving unsolicited electronic mail messages.

{18} A private actor, however, may be viewed as a state actor under two situations. First, the private actor has to perform an exclusive public function.[59] In *CompuServe Inc. v. Cyber Promotions, Inc.*, Cyber Promotions alleged that CompuServe, by providing Internet e-mail service to its subscribers, was acting as a postmaster,[60] which is a function that has been performed traditionally by the state. This argument, however, is attenuated at best because the state does not have the exclusive prerogative, ability, nor interest to furnish all of its constituents with Internet access. As previously stated, the Internet has been determined to be a decentralized mode of communication.[61] Unlike the United Stated Postal Service, Internet e-mail service is not provided by any one entity.[62] Furthermore, e-mail service is not readily accessible to the

general public because only a portion of society owns a computer or has access to one that is capable of sending and receiving e-mail messages. In addition, only a portion of those with Internet service actually use electronic mail as a means of communication.

{19} To prevail on the argument that Internet service providers are performing an exclusive public function, solicitors must show that Internet service providers are "performing the full spectrum of municipal powers and [is standing] in the shoes of the State."[63] The court in *Cyber Promotions, Inc. v. America Online, Inc.* proclaimed that by supplying the public with access to the Internet, the ISP was neither executing any municipal powers nor standing in the shoes of the state.[64] The same proclamation can be applied to almost all other Internet service providers, which are in a position nearly identical to that of AOL's. Internet service providers may gain a higher probability of being depicted as standing in the shoes of the state if "the network . . . assume[s] a wider variety of [state] attributes."[65] Even if the government began using the network to perform traditional state functions, such as providing methods for their constituents to cast votes, the courts would not likely scrutinize an online service provider as a state actor because it merely furnishes the means which allows the government to perform a state function. CompuServe has not performed an exclusive public function that would change its status from a private actor to a state actor.

{20} Secondly, for a private entity to be viewed as a state actor, it has to become entangled with a state actor. The entanglement argument has two prongs, neither of which has any direct bearing on Internet service providers. The first question the courts ask is whether state officials have helped or acted in concert with an ISP in providing Internet access service.[66] The courts then consider whether states and Internet service providers are interdependent entities, thereby making them joint participants in the service of providing Internet access to the public.[67] Courts that have addressed these questions have answered them in the negative.[68]

{21} The government only has a minor and indirect connection to Internet service providers such as AOL and CompuServe. Although the government has allowed its computers and computer networks to be linked with the Internet, "the government apparently does not plan to operate the networks."[69] In fact, government literature emphasizes that "'[t]he private sector will lead the deployment of the [National Information Infrastructure] and 'the private sector role in NII development will predominate.'"[70] The government has not influenced nor been involved in the business decisions of these ISPs. The court in *America Online, Inc.* held that the lack of participation was sufficient in declaring that the government was not a joint participant.[71] Furthermore, although some ISPs have sought the aid of federal courts, the simple fact that a suit has been filed in federal court does not signify involvement with a state actor.[72] For a private and state actor to be intertwined so that their division is not distinguishable, the state actor has to be intimately involved with the activities of the private actor. The peripheral role of the government with respect to Internet service and access does not amount to entanglement or interdependence.

{22} Assume, however, the spammers prevailed in showing that Internet service providers are state actors and any restrictions on spamming, either by use of filtration/blocking software or by order of an injunction, amounts to a form of governmental regulation.[73] Nonetheless, First Amendment guarantees are not absolute. A business does not have an inviolable right to commercial speech.[74] Businesses do not have the right to demand acceptance of their advertisements by everyone to whom the advertisements are sent. "[The] mailer's right to communicate must stop at the mailbox of an unreceptive addressee . . . . To hold less would be to license a form of trespass..."[75] Numerous complaints from subscribers indicate that many are unhappy receiving the unsolicited electronic mail advertisements. Subscribers have threatened to end their enrollment if the spamming does not stop.[76] Therefore, before a court can declare a business has the right to send unsolicited mail, the court may face the tedious task of balancing the business's right to freedom of speech with the individual's right of privacy.

{23} Fundamental rights granted by the Constitution are not absolute guarantees; therefore, "the right of

every person 'to be left alone' must be placed in the scales with the right of others to communicate."[77] Traditionally, courts have vigorously protected freedom of speech. The argument, however, can be made that a spammer's right to communicate would not be unduly burdened by a restriction on unsolicited mass e-mails because effective alternative means of communication are available.[78]For example, spammers may advertise through use of online bulletin boards, the World Wide Web, postal mail, telemarketing, and newspapers.[79] Considering the alternative means of advertising available, ISP subscribers should not be forced to accept unwanted e-mail. Additionally, because the survival of Internet service providers is dependent upon the volume of their membership, they should not lose business when adequate alternatives exist which could lessen the burden on them and their subscribers.

{24} This discussion merely illustrates the analysis that the courts would undergo if ISPs were state actors. Notwithstanding the above discussion, spammers cannot rely on freedom of speech as an effective defense because ISPs are not state actors.[80]

{25} If challenged in court, statutes which attempt to regulate spam will survive judicial scrutiny. If federal and state legislatures enact a statute to regulate spam, courts will use the *Central Hudson/Fox* standard of scrutiny to analyze the validity of the challenged statute.[81] Spammers might argue that most unsolicited e-mail messages neither mislead[82] nor advertise illegal activity. The government interest in protecting the privacy of ISP customers, preserving the integrity of the Internet, and minimizing the burden on ISPs' computer systems may not be considered substantial enough to outweigh the right to freedom of commercial speech. Moreover, government regulation must be narrowly tailored and directly advance a government interest. Those are among the arguments that spammers may assert, perhaps with little chance of success, to challenge the constitutionality of a statute regulating or prohibiting spam. If challenged, the state or federal statute will face some difficult hurdles before the courts will declare it a valid restriction of commercial speech. The proposed bills discussed in Part V of this article may be scrutinized under the *Central Hudson/Fox* standard if they are challenged in court.[83]

III. Other Defenses Asserted by Spammers

A. *Essential Facilities Defense*

{26} In addition to the free speech defense discussed above, spammers have asserted an essential facilities defense. The essential facilities doctrine states that "a business or group of businesses which controls a scarce facility has an obligation to give competitors reasonable access to it."[84] Spammers contend that ISPs control a scarce facility; as such, spammers argue that they, as competitors, have the right to reasonable access of the essential facility.[85] One court, however, already has determined that ISPs are not essential facilities.[86]

{27} In *America Online, Inc. v. Cyber Promotions, Inc.*,[87] AOL implemented blocking software to which Cyber Promotions objected. The new software is designed to prevent AOL's subscribers from receiving e-mail from a sender whose e-mail address has been put on a list of domain names and Internet Protocol addresses maintained by AOL. AOL places spammers on this list if they have been the subject of complaints by AOL subscribers and if they have refused to stop sending spam. Cyber Promotions contended that the use of this software violates federal antitrust laws because AOL is an "essential facility," which requires it to allow its competitors to have reasonable access to its facilities. Ruling that AOL was not an essential facility, the court denied Cyber Promotions' motion for preliminary injunction against use of this blocking software.[88]

{28} The driving force behind the "essential facilities" doctrine is the desire to prevent monopolies. Normally when a company attains monopoly or oligopoly power, there is cause for public concern because that

company serves a substantial part of the general public. Courts must look at the good or service provided, the threat of competition, and the presence of government regulation.[89] To be a monopoly, the business entity must have a monopoly power, which necessarily includes the power to set higher than competitive prices for the goods or services. AOL, however, does not have the privilege of charging its subscribers monopoly prices because other competitors are present in the market. If AOL were to charge more than the competition, its subscribers would switch to another Internet service provider. Furthermore, AOL clearly does not enjoy monopoly power because of the availability of many competitive ISPs, such as CompuServe, Erols, Prodigy, and Microsoft Network, as well as local ISPs. Subscribers to any of these ISPs may switch freely from one service provider to another. In addition, new competitors can easily gain entry into this market with only a small amount of capital. Consequently AOL, by supplying e-mail access, does not maintain sufficient control of the market to constitute monopoly power.[90]

{29} The "essential facilities" defense fails for another reason: ISPs and spammers are not competitors. ISPs provide their subscribers with Internet access. Spammers advertise various goods and services. The fact that spammers advertise via e-mail messages does not place them in competition with ISPs. Rather, spammers rely on the service provided by these ISPs in order to send their unsolicited advertisements via e-mail. Spammers and Internet service providers can be considered competitors only in the sense that they hold opposing positions with respect to unsolicited e-mails. Spammers want to continue sending unsolicited e-mails, whereas Internet service providers want to prohibit them. A spammer's true competitor would be another entity that engaged in the business of providing advertising via e-mail.

B. *Public Utility Defense*

{30} Spammers have also put forth a public utility defense. To be classified as a public utility, ISPs must meet three elements. First, they must possess an essential good or service to which the general public has a legal right to demand or receive; second, the service must be provided indiscriminately; third, its business of providing the service must concern the public.[91] The public utility defense fails for two reasons. First, providing Internet access is not an essential service because there are alternative channels of communication that a company can use to send unsolicited advertisements, such as television, the United States mail and newspapers. Second, the court will consider whether the ISP maintains a monopolistic or oligopolistic position with regard to providing Internet access. As previously stated, commercial online computer services are not monopolies or oligopolies.[92]

{31} Applying the above analysis, the court in *CompuServe Inc. v. Cyber Promotions, Inc.* held that CompuServe was not a public utility.[93] Consequently, Cyber Promotions did not have a legal right to demand use of CompuServe's computer services. The court determined that CompuServe did not provide an essential service because there were alternative modes of communication available to the general public. The court further pointed out that CompuServe's services are not readily used by the general population.[94] Therefore, CompuServe was not a public utility.

IV. Judicial Developments

A. *Cyber Promotions, Inc. v. Apex Global Information Services, Inc.*

{32} In addition to *CompuServe Inc. v. Cyber Promotions, Inc.*[95] and *America Online, Inc. v. Cyber Promotions, Inc.*,[96] discussed above, this section will review several subsequent cases. In *Cyber Promotions, Inc. v. Apex Global Information Services, Inc.*,[97] the court faced a different type of spamming issue than in the previous cases. In that case, the court enforced a contract entered into between Cyber Promotions and Apex Global Information Services, Inc. ("Apex"), an Internet Service Provider ("ISP"). Apex contracted to provide Cyber Promotions with access to the Internet. Apex knew that Cyber Promotions was in

the business of sending unsolicited e-mail advertisements. Moreover, Apex agreed not to terminate Cyber Promotions subscription without thirty days' notice. Cyber Promotions' advertising techniques ultimately consumed a large portion of Apex's computer resources; consequently, Cyber Promotions' subscription was terminated without thirty days' notice. Accordingly, Cyber Promotions filed suit for breach of contract.[98]

{33} The court held that Cyber Promotions' claim for breach of contract was valid and enjoined Apex from terminating Cyber Promotions' subscription.[99] The court noted that, although unsolicited e-mail messages are undesirable, and that Cyber Promotions' actions are controversial, "the fact that Cyber [Promotions] is an unpopular citizen of the Internet does not mean that Cyber [Promotions] is not entitled to have its contracts enforced in a court of law."[100] The court knew that reactivation of Cyber Promotions' subscription would result in great damage to Apex, Apex's clients, and to other Internet users, but the court blamed Apex's conduct for its decision.[101] Knowing the nature of Cyber Promotions' business, Apex freely contracted not to terminate Cyber Promotions' subscription without thirty days' notice. Apex subsequently terminated Cyber Promotions' subscription without the required notice. Given these facts, the court had no choice but to reactivate Cyber Promotions' subscription because there was a clear breach of contract.

B. *People v. Lipsitz*

{34} *People v. Lipsitz*[102] is different from almost all other Internet cases because it was filed in the Supreme Court of New York County, as opposed to a federal court. Therefore, in dealing with the jurisdictional issue, the court held that it could hear the case because the spammer was selling magazine subscriptions in the state of New York via e-mail through a local ISP.[103] Moreover, the spammer was physically located in New York and the acts complained of occurred in New York.

{35} Kevin Jay Lipsitz, a magazine salesperson, advertised subscriptions to various magazines by sending mass e-mails to New York residents. Lipsitz falsified the return address on those e-mails so that they could not be traced back to him. The contents of the e-mails were also false. The messages indicated that they were written by a satisfied customer and that subscriptions were obtained by referral and not by solicitation. In actuality, those who subscribed never received their magazines or received them for only a portion of the subscription term.[104]

{36} The court's holding was specific to the facts of this case and cannot be applied broadly. The court enjoined Lipsitz's actions based on a charge of false advertising and on a charge of operating under an unfiled business name.[105] Surprisingly, however, the court held that falsifying the return address of an e-mail message was merely a method "designed to inspire confidence" in the content of the e-mail.[106]

D. *Parker v. C.N. Enterprises*

{37} In *Parker v. C.N. Enterprises*,[107] C.N. Enterprises ("C.N.") sent unsolicited e-mail messages using Tracy Parker's domain name as the return address. Many of the e-mails that were sent had invalid addresses and were returned to Parker's address because C.N. was using her domain name. As a result, Parker and her Internet service provider, Zilker Internet Park, Inc. ("Zilker"), filed suit against C.N.[108]

{38} The court permanently enjoined C.N. from sending unsolicited e-mail using Parker's domain name.[109] The court reasoned that C.N.'s actions amounted to a trespass and nuisance because it was not entitled to the use of Parker's domain name.[110] Surprisingly, the court enjoined C.N. from sending unsolicited e-mail using any other domain name without express permission from the owner of that domain name.[111] Furthermore, the court found that C.N.'s actions "inflicted substantial harm [on Parker and Zilker], including substantial service disruptions, lost access to communications, lost time, lost income and lost opportunities."[112] C.N. also caused harm to Zilker's system, which was temporarily disabled from the exhaustion of its processing and storage facilities.[113]

{39}Countless other complaints have been filed against spammers, some of which are pending in court,[114] and some of which have been settled out of court. Until legislation is enacted restricting the intrusiveness of spam, many more complaints will be filed against spammers in the future.

V. Legislative Developments

A. *Federal Legislation*

{40} The courts' trend to enjoin spamming may have spurred federal and state legislatures to action. Legislators have introduced many bills in Congress, but none have been enacted. Because the Internet is a "decentralized, global medium of communications,"[115] a federal statute would be more effective in regulating spam than disparate and varied state statutes.

{41} Currently, Congress is considering seven bills purporting to regulate unsolicited e-mail. None of the bills proposes to ban completely the use of e-mail as a method of unsolicited communications. On the other hand, all seven bills require that the unsolicited e-mail contain the sender's name, street address, telephone number, and e-mail address.[116] That provision is important for two reasons. First, the provision would allow the recipient to identify the spammer, so that innocent third parties will not be blamed for the actions of spammers, as in *Parker v. C.N. Enterprises*.[117] Second, the provision would allow effective use of filtration software implemented by ISPs, which would be able to identify and block certain domain names. However, knowledge of the spammer's e-mail address would prove more helpful to the ISPs, especially if the spammer is required to honor a recipient's request to be removed from the spammer's mailing list. Only one of the seven pending bills does not require spammers to honor a recipient's request to terminate further communication.[118]

{42}A couple of the pending bills have distinct provisions worth noting. House Bill 4124 contains a provision that makes it unlawful for any person to send an unsolicited commercial e-mail message to subscribers of an Internet service provider if the spammer "know[s] or [has] reason to know that such action is in contravention of the rules of the interactive computer service."[119] This bill places the burden on the ISP to establish a policy prohibiting spam. If the ISP lacks such a policy, then the spammer cannot be held accountable for his actions.

{43} Senate Bill 771 has two important features. First, this bill requires that spamming parties label each unsolicited commercial e-mail an "Advertisement."[120] Secondly, the bill states that upon subscriber demand, the Internet service provider has to implement a filtration software that blocks the subscriber's receipt of e-mails which have the word "Advertisement" in the subject line of the message.[121] This bill differs from other bills because, in addition to imposing a duty on the spammer, it also imposes a burden on the recipient's Internet service provider to filter incoming e-mail messages.

B. *State Legislation*

1. State Legislation Passed

{44} Only a handful of states have passed legislation to regulate spamming. The problem with state regulation of spam is that the application of the statute has jurisdictional boundaries. Consequently, spammers who have no connection to the states of California, Nevada, or Washington will not be affected by the regulations of those state statutes.

{45} Assembly Bill 1629 was passed by the California Legislature on August 27, 1998.[122] Like House Bill 4124 discussed above, Assembly Bill 1629 imposes the burden of regulating spam on the individual Internet

service providers. The bill does not require spammers to include their name, street address, telephone number, and electronic mail address on each unsolicited e-mail as required by all seven bills currently pending in Congress. Rather, Assembly Bill 1629 prohibits an ISP's subscriber from using such service provider's equipment to transmit unsolicited e-mail if the ISP's published policy forbids such actions.[123] In addition, the legislation requires that no person receive permission to use the equipment of an Internet service provider in the dissemination of unsolicited e-mails if the service provider's published policy forbids such actions.[124] Accordingly, Assembly Bill 1629 imposed two burdens on ISPs. First, they have a burden to established and publish a policy against unsolicited e- mail. Second, they have the burden to bring suit if a spammer has violated their published policy.

{46} Assembly Bill 1629 may not be an effective remedy in the fight against spam given the past actions of spammers. Most ISPs have published policies that prohibit the use of their equipment to disseminate unsolicited e-mail. Those policies have not thwarted the actions of many spammers. For example, Cyber Promotions continued to send spam to AOL's subscribers even though AOL has an explicit policy against spamming. In fact, Cyber Promotions continued to send spam even after AOL had requested that they stop. Assembly Bill 1629 has done nothing to increase a recipient's ability to choose whether or not he or she wants to receive unsolicited e-mails.[125] Part VII of this article will suggest that government regulation put the power of control in the hands of ISP subscribers.

{47} Nevada was the first state to pass a bill regulating spam, Senate Bill 13, which became effective July 1, 1998. This bill is similar to House Bill 1748 in that it prohibits the transmission of unsolicited e-mail messages unless the sender has a preexisting business relationship with the recipient.[126] Absent such a relationship, the spammer may send an unsolicited e-mail only if the message can be identified as an advertisement and only if the message includes the sender's name, address, electronic mail address, and instructions on how to remove the recipient's name and e-mail address from future mailing lists.[127] This bill differs from California's Assembly Bill 1629. Senate Bill 13, under most circumstances, allows the recipient of spam to retain control over what he or she blocks.

{48} Finally, the State of Washington passed a bill regulating spam on March 25, 1998, which became effective June 11, 1998. House Bill 2752 prohibits a person or other entity from sending unsolicited e-mail messages that contain a false return address or that contain incorrect information as to the origin of the e-mail.[128] The bill further provides that a person or other entity cannot use a third person's domain name without that person's permission.[129] In addition, the bill states that the subject line of an unsolicited e-mail cannot have falsified or misleading information.[130] Of the three bills passed by state legislatures, Washington's House Bill 2752 gives e-mail recipients the most control over whether or not they wish to receive spam.[131]

{49} Several other states are proposing to regulate spam. Some states that have bills regulating spam pending in their respective state legislatures include Alaska,[132] Kentucky,[133] Maryland,[134] Massachusetts, [135] New Jersey,[136] New York,[137] North Carolina,[138] Rhode Island,[139] Virginia,[140] and Wisconsin.[141] Of the ten states that have proposed bills to regulate spam, Alaska, Kentucky, North Carolina, and New York would require the spammer to provide information identifying it as the sender. Moreover, the bills proposed by those four states would require that spammers allow the recipients an option to decline receipt of future spam. Alaska, North Carolina and New York also require the spammer to identify the message as an advertisement. Some states, such as Maryland, Massachusetts, New Jersey, Rhode Island, and Wisconsin, have proposed legislation that would prohibit the dissemination of unsolicited advertisements via e-mail. If those prohibitions against spam pass their legislatures, affected spammers undoubtedly will challenge the constitutionality of the statutes in court. At that time, the court will have to apply the *Central Hudson/Fox* standard of scrutiny in assessing the constitutionality of any statutes prohibiting or regulating spam.[142]

{50} Conversely, three other states rejected bills regulating spam. Colorado enacted House Bill 1284,[143] but before its enactment, the state legislature deleted the provision regulating spam.[144] The amended bill only regulates fax solicitations. Connecticut proposed a bill to prohibit spam, but its senate never took action on it.[145] New Hampshire also proposed a bill regulating spam, but the bill died in New Hampshire's house.[146]

{51} Both federal and state lawmakers have taken note of problems associated with spam: spam-related litigation has encouraged those lawmakers to act. Although effective regulations against spam still are lacking, it almost is certain that some regulation will be enacted within the coming years.

VI. Legal Theories Used By Internet Service Providers

A. *Trespass to Chattel*

{52} Legislative regulation is currently unavailable to ISPs who do not conduct business in California, Nevada or Washington. As such, most ISPs still must rely on the judicial system to enjoin spamming. Several claims can be brought against a spammer.

{53} The first claim is trespass to chattels. The Internet is still emerging as a widely used tool of communication; consequently, few laws currently govern trespass in cyberspace. The crime of trespass to chattel requires an overt act with the intent to interfere with a chattel in the possession of another, thereby resulting in actual damages to the chattel. "Thus[,] it is a trespass to damage goods or destroy them, [or] to make an unpermitted use of them."[147] Presently, "computer hacking" is considered to be a form of trespass.[148] Computer hacking occurs when a person intentionally gains access to another's computer system without authorization.

{54} Many ISPs have filed suit against spammers alleging trespass to chattel. These ISPs allege that spammers have intentionally, and without authorization, used the service providers' equipment to disseminate unsolicited e-mail messages that impaired the ISPs' equipment and deprived their subscribers of the legitimate use of their equipment.[149] The claim that spamming is a trespass appears to be gaining legitimacy. The court in *CompuServe Inc. v. Cyber Promotions, Inc.*[150] granted the Internet service provider a preliminary injunction based partially on the theory of trespass. Moreover, the court in *Parker v. C.N. Enterprises*[151] ruled for the plaintiffs on their trespass claim.

B. *Computer Fraud and Abuse Act*

{55} ISPs also have used the Computer Fraud and Abuse Act ("CFSA") as a vehicle for their complaints against spammers. [152] In relevant part, 18 U.S.C. § 1030(a)(5)(A) prohibits a person from "knowingly caus[ing] the transmission of a program, information, code, or command to a computer or computer system."[153] This prohibition applies to a person who intends the transmission to "damage, or cause damage to, a computer, computer system, network, information, data, or program; or . . . withhold or deny, or cause the withholding or denial, of the use of a computer, computer services, system or network, information, data or program."[154] In addition, the transmission must occur "through means of a computer used in interstate commerce or communications" and without the ISP's authorization.[155] And finally, the Code provides that the damage to the Internet service provider for any one year period must aggregate at least $1,000.[156]

{56} Spam can have the effect of disabling a computer system because "[h]igh volumes of junk e-mail devour computer processing and storage capacity [and] slow down data transfer between computers over the Internet by congesting the electronic paths through which the messages travel."[157] The congestion of the computer system would deny both ISPs and their subscribers use of the system. Mass volumes of spam can

also cause damage to the ISP's computer system because most service providers have mail systems which have a finite capacity to process and store e-mail. Accordingly, "[t]he mail system is not designed to accommodate, and it is vulnerable to disruption by, indiscriminate mass mailings from . . . senders of unsolicited commercial e-mail."[158] Consequently, the ISP will not face a problem in proving damages.

{57} Even though ISPs have the arduous burden of proving damages, they also have the more difficult burden of proving that the spammer intended to cause the damage as stated in the above paragraph. In light of the recent and abundant controversy regarding spam, however, it may be difficult for a spammer to deny that its actions resulted in damages to the ISP's computer system.

C. *False Designation of Origin*

{58} Several claims are available to an ISP whose domain name was used falsely by the spammer as its electronic return address. One such claim falls under 15 U.S.C. § 1125(a)(1)(A). This code section prohibits any person from:

> us[ing] in commerce any word, term, name, symbol, or device, or any combination thereof, or any false designation of origin, false or misleading description of fact, or false or misleading representation of fact, which [A] is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person . . . .[159]

{59} Generally, ISPs do not want to be associated with spam, much less the product or service that is being advertised.[160] The majority of the population who communicates via electronic mail abhors spam; therefore, ISPs do not want to portray the image that they tolerate spam in any sense. As such, ISPs and other plaintiffs argue that when a spammer uses the service provider's domain name in the electronic return address of the unsolicited e-mail, such usage not only causes confusion but also leads the recipient to believe that the ISP tolerates, condones, or endorses the spammer's advertised product or service or that the ISP is somehow "affiliated, connected or associated"[161] with the spammer. Those beliefs by the recipient can damage the name and reputation of the ISP and other third-party plaintiffs, whose domain name is being used is spam.

{60} Additionally, ISPs have several others claims of which they may avail themselves. Several ISPs have filed suit alleging dilution of interest in service mark pursuant to 15 U.S.C. § 1125(c)(1), violation of the Electronic Communications Act pursuant to 18 U.S.C. § 2701, unfair competition, unjust enrichment, and misappropriation of name and identity.

{61} Although an ISP has several avenues with which to seek relief in a court of law, relief is not certain. So far, courts have been sympathetic to the plaintiffs, which necessarily includes ISPs, but an injunction is not guaranteed and the judicial process is slow. Several of the cases, particularly those involving Cyber Promotions, have resulted in settlement. For the moment, however, most ISPs have no choice but to rely on the courts to enjoin the actions of spammers.

VII. Recommendation

{62} Although commercial online computer service providers and other plaintiffs have prevailed in court, these are small victories. These plaintiffs may not be as fortunate with the next spammer who comes along. The court must make a case-by-case determination of whether a wrong has been committed and whether the spammer will be allowed to continue its practice. To avoid the uncertainty of a case-by-case determination, government regulation is needed. The fight against spam cannot be fought by the private online services

alone. These entities have tried sending letters to the spammers requesting them to stop, implemented blocking software, written explicit prohibitions against spamming in their contractual agreement with members, and even sent "e-mail bombs". These attempts, however, will not be successful without the help of government regulation. Moreover, "the online giant[s] [are] increasingly taking [their] cases to the court system, where judges have been sympathetic so far."[162] This increasing reliance on litigation to resolve the matter is backing up court dockets. The government should stop dragging its feet and step up to the plate to relieve the courts of some of the burden of deciding spamming cases. Although legislation has been proposed, none have been passed.

{63} As discussed in Part II.D of this article, although a complete ban on sending unsolicited commercial advertisements via e-mail may not survive the intermediate standard of review, less drastic governmental regulations could be imposed. As one court has stated, "the Internet is one of those areas of commerce that must be marked off as a national preserve to protect users from inconsistent legislation that, taken to its most extreme, could paralyze development of the Internet altogether."[163] This is a result that no one wants to see. In drafting regulations, the government should look to the settlement that took place between AOL and Cyber Promotions on January 31, 1997, which allows AOL subscribers to choose whether or not they want to receive unsolicited e-mail.[164]

{64} Consequently, the best solution may be to increase user control and decrease governmental regulation. Because the Internet is already a decentralized medium of communication, an increase in user control may reduce the need for government regulation.[165] A reduction in governmental regulation does not mean a complete lack of governmental regulation. User control requires: "(1) [a] means of identifying the content being transmitted, and (2) the ability of the user to screen out certain kinds of content."[166] Blocking software is useless if the header of an e-mail message is disguised. To allow users of the Internet to control materials that enter their e-mail boxes, the government needs to impose a regulation prohibiting spammers from falsifying the return address of the unsolicited e-mail message.[167] If the return address is incorrect, then the receiver is unable to send a response e-mail requesting that his or her e-mail address be deleted from the spammer's mailing list, thereby inhibiting user control.

{65} That was the approach taken in the settlement agreement between Americal Online and Cyber Promotions on January 31, 1997. The settlement is a relief for Cyber Promotions, which was denied a temporary restraining order on AOL's use of its blocking and filtration software on November 26, 1996.[168] The court also granted summary judgment on November 4, 1996, on Cyber Promotions' First Amendment claim.[169] The settlement imposes an obligation on both AOL and Cyber Promotions. Cyber Promotions can use only a limited number of domains from which it can send unsolicited e-mail advertisements.[170] The imposition of this limitation will allow AOL subscribers effectively to block e-mails that are derived from certain domain names.[171]

{66} In the past, Cyber Promotions averted this blocking tool by frequently changing its domain names. On the other hand, AOL is obligated to inform its subscribers that the blocking software allows them to choose to receive unsolicited e-mails.[172] Subscribers have the option to unblock those domain names from which they want to receive unsolicited e-mails. Both AOL and Cyber Promotions have referred to this settlement as a victory. Stanford Wallace, President of Cyber Promotions, stated that "'[t]his was a business model that we were considering . . . . This way we know the mail is going to people who want it.'"[173] Furthermore, David Phillips, associate general counsel of AOL, proclaimed that "'[t]his decision is a big win for AOL members because it puts them in control of their email. They can still receive Cyber Promotions junk email if they want.'"[174] Some of the bills proposed by Congress do require that spammers provide recipients with their electronic return address. To this day, however, none of these bills have been passed.

{67} In addition, the government should impose a law that requires the senders of unsolicited commercial advertisements to accurately label the nature of their communication. Essentially, this requirement demands

that the word "Advertisement" be included in the subject line of the electronic mail message. Only one of the bills proposed by Congress, Senate Bill 771, required the spammer to label their unsolicited message as an "Advertisement."[175] This requirement is needed as a secondary means by which recipients can exert control over what they spend time reading. Undoubtedly, blocking and filtration software cannot weed out all unsolicited e-mails. Old spammers may switch domain names or new spammers may bring in new domain names which will not be picked up by the blocking and filtration software. Clear identification of the nature of the e-mail will allow recipients to delete unsolicited e-mails before they spend their valuable time opening and reading the message.

{68} Moreover, the government could restrict online services from selling profiles on their members, which may include the subscribers' e-mail addresses, hobbies, and interests.[176] A regulation that restricts the sale of personal information potentially would not invoke any First Amendment concerns because what is being regulated is conduct not speech.[177] These three proposed regulations will help users of the Internet exercise some autonomy over what they do and do not receive.

VIII. Conclusion

{69} The Internet can be an invaluable means of research and communication. The Internet allows people all over the world to communicate instantly, conveniently, and cheaply. Electronic information can be transmitted through cyberspace faster than any other means of transmission currently in existence. The future of this magnificent network may be in jeopardy if the government does not get involved in regulating spam. Internet users may find it more burdensome to scroll through and erase "junk e-mail" than the system is worth.

{70} Presently, the law is clear that a business's right to send unsolicited commercial advertisements via electronic mail is not protected by the First Amendment of the Constitution. In the near future, the only remedy available to those who cannot benefit from California, Nevada, or Washington's spamming laws against spam may be to bring a civil suit in a court of law. The court may be willing to declare the spamming a trespass where the spammer ignores warning letters and evades filtration software, as it did in *Parker v. C.N. Enterprises*[178] and in *CompuServe Inc. v. Cyber Promotions, Inc.*[179] The court may be willing to enjoin the actions of the spammers on other counts, such as a violation of the Computer Fraud and Abuse Act. Regardless of the remedies available to Internet service providers in the judicial system, it remains necessary for legislatures to enact regulations that serves the interest of all parties involved by increasing user control.

[**] **NOTE:** All endnote citations in this article follow the conventions appropriate to the edition of THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION that was in effect at the time of publication. When citing to this article, please use the format required by the Seventeenth Edition of THE BLUEBOOK, provided below for your convenience.

Cathryn Le, Note, How Have Internet Service Providers Beat Spammers?, 5 RICH. J.L. & TECH. 9, (Winter 1998), *at* http://www.richmond.edu/jolt/v5i2/le.html.

[*] Cathryn A. Le earned her B.A. in Economics at the University of Virginia, Charlottesville, Virginia. Currently, she is a third-year law student at the University of Richmond, T.C. Williams School of Law, Richmond, Virginia. Ms. Le is the 1998-1999 Annual Survey Editor of the *University of Richmond Law*

Review.

[1] American Civil Liberties Union v. Reno, 929 F. Supp. 824, 831 (E.D. Pa. 1996), *aff'd* 521 U.S. 844 (1997).

[2] *See* Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp. 456 (E.D. Pa. 1996).

[3] *See Reno*, 929 F. Supp. at 832.

[4] *See id*. at 831.

[5] *See Reno,* 929 F.Supp. at 833.

[6] *Id*. at 831.

[7] *See* Michael W. Carroll, *Garbage In: Emerging Media and Regulation of Unsolicited Commercial Solicitations*, 11 Berkeley Tech. L. J. 233, 234 (1996).

[8] Those who send unsolicited electronic mail advertisements are known as "spammers" and collectively will be referred to as such throughout this article. *See id*. at 253. In addition, the act of sending unsolicited electronic mail messages occasionally will be referred to in this article as "spamming." *See id*.

[9] *Id*.

[10] *See id*. at 255

[11] Most cases seeking an injunction on unsolicited e-mails are filed by Internet service providers, such as America Online, Inc. *See, e.g*., Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp. 456 (E.D. Pa. 1996). Some cases, however, have been filed by individual Internet users. *See*, *e.g*., Complaint, Seidl v. Greentree Mortgage Co. (D. Colo. 1997) (visited Jan. 19, 1999) <http://www.cs.colorado.edu/~seidl/lawsuit/complaint.html> [hereinafter Seidl Complaint].

[12] This article will address unsolicited commercial electronic mail messages, which does not include unsolicited political communications or charitable solicitations.

[13] Fred H. Cate, *The First Amendment and the National Information Infrastructure*, 30 Wake Forest L. Rev. 1, 9 (1995) (emphasis added) (citation omitted) (quoting New York Times Co. v. Sullivan, 376 U.S. 254, 269 (1964)).

[14] Alex Kozinski & Stuart Banner, *Who's Afraid of Commercial Speech?*, 76 Va. L. Rev. 627, 628 (1990) (quoting Valentine v. Chrestensen, 316 U.S. 52, 54 (1942)).

[15] U.S. Const. amend. I. The First Amendment of the Constitution states in pertinent part: "Congress shall make no law . . . abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." *Id*.

[16] *See generally* Breard v. Alexandria, 341 U.S. 622, 644-45 (1951) (balancing the right of privacy against the publisher's right to distribute publications door to door).

[17] Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, 425 U.S. 748, 770 (1976).

[18] *See* Central Hudson Gas & Electric Corp. v. Pubic Service Comm'n, 447 U.S. 557, 563 (1980). Since

this decision, "the Court has granted commercial speech some protection, although considerably less than other sorts of speech. But the concept of a commercial/noncommercial distinction has remained in the law." Kozinski & Banner, *supra* note 15, at 628.

[19] *See* Carroll, *supra* note 8, at 238.

[20] 447 U.S. 557 (1980).

[21] *See* Carroll, *supra* note 8, at 238 (citing Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n, 447 U.S. 557, 564-65 (1980)).

[22] *See id*. (citations omitted).

[23] *Id*.

[24] *Id*. (quoting Board of Trustees v. Fox, 492 U.S. 469, 480 (1989)).

[25] *See* Rowan v. United States Post Office, 397 U.S. 728 (1970).

[26] *See* Carroll, *supra* note 8, at 239.

[27] *See id*. at 249.

[28] *See* Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227(b)(1)(B) (1994); Moser v. Federal Communications Comm'n, 826 F. Supp. 360 (D. Or. 1993), *rev'd*, 46 F.3d 970 (9th Cir. 1995).

[29] 47 U.S.C. § 227(b)(1)(C).

[30] 844 F. Supp. 632 (D. Or. 1994).

[31] *See id*. at 634.

[32] *See id*. at 636.

[33] *See* Carroll, *supra* note 8, at 253.

[34] *Id*. at 261.

[35] Several online service providers have alleged a strain that their mail servers suffer from processing mass electronic mail messages. Mail servers have finite capacity and, therefore, are unable to process mass mailings. *See, e.g.*, America Online's Complaint, America Online, Inc. v. Over the Air Equipment, Inc. (E.D. Va. 1996) (No. 96-462) (visited Jan. 19, 1999) <http://www.ljx.com/LJXfiles/aol/aolsuit.html> [hereinafter America Online's Complaint I]; America Online's Complaint, America Online, Inc. v. Prime Data Systems, Inc. (E.D. Va. 1997) (visited Jan. 19, 1999) <http://www.jmls.edu/cyber/cases/aol-pd0.html> [hereinafter America Online's Complaint II].

[36] Several online service providers allege that their staff spends to much time routing and re-routing mass e-mails, and that the resources and time spent processing these e-mails delays the receipt of legitimate e-mail by paying subscribers. *See* America Online's Complaint I; America Online's Complaint II; Complaint, Juno Online Services, L.P. v. Scott Allen Export Sales (S.D.N.Y. 1997) (No. 97-8694) (visited Jan. 10, 1999) <http://www.jmls.edu/cyber/cases/juno/comp.html> [hereinafter Juno's Complaint I].

[37] *See* Destination Ventures, Ltd. v. Federal Communications Comm'n, 844 F. Supp. 632, 636 (D. Or.

1994).

[38] *See* CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1019 (S.D. Ohio 1997); America Online's Complaint I, *supra* note 36; America Online's Complaint II, *supra* note 36; Juno's Complaint I, *supra* note 37, at 9.

[39] *Destination Ventures*, 844 F. Supp. at 636.

[40] Mark Eckenwiler, *Just the Fax, Ma'am*, Netguide (1996).

[41] *Id*.

[42] *See* 47 U.S.C. § 227(b)(1)(C) (1994).

[43] 948 F. Supp. 436 (E.D. Pa. 1996).

[44] Cyber Promotions, Inc. is an advertising agency that sends numerous unsolicited e-mail advertisements on behalf of itself and its clients.

[45] Nine cases have been filed against Cyber Promotions, Inc. for its practice of sending unsolicited electronic mail messages. *See Unsolicited E-mail: Cases* (visited Jan. 10, 1999) <http://www.jmls.edu/cyber/cases/spam.html>.

[46] 948 F. Supp. 436 (E.D. Pa. 1996).

[47] *See id*. at 437.

[48] *See id*.

[49] *See id*. The sending of a mass number of e-mails at one time is referred to as an "e-mail bomb." *See id*. at 436 n.1.

[50] *See id*. at 437.

[51] *See id*. at 436.

[52] 962 F. Supp. 1015 (S.D. Ohio 1997).

[53] In November 1996, CompuServe received 9970 complaints from their subscribers concerning unsolicited e-mails, of which 50 per day mentioned Cyber Promotions specifically. *See id*. at 1023. At the present time, only a small number of Internet users choose to pay an hourly rate as opposed to a flat monthly rate; therefore, Cyber Promotions would not be shifting any direct costs of advertising to their recipients but there are indirect costs involved.

[54] *See id*. at 1028.

[55] *See* Hudgens v. NLRB, 424 U.S. 507, 513 (1976); *see generally*, Hurley v. Irish-American Gay Group, 515 U.S. 557 (1995).

[56] *See, e.g., CompuServe, Inc*., 962 F. Supp. at 1026 (holding that CompuServe was a private actor); Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp. 436, 443-45 (E.D. Pa. 1996) (holding that AOL was not a state actor).

[57] *See, e.g., America Online, Inc.*, 948 F. Supp. at 456 (denying the solicitor a preliminary injunction against AOL's use of a blocking software).

[58] *See, e.g., CompuServe*, 962 F. Supp. at 1019 (acknowledging that CompuServe had created a filtration system but did not rule as to its legality because the solicitor did not allege an antitrust claim).

[59] *See* Mark v. Borough of Hatboro, 51 F.3d 1137, 1142 (3d Cir. 1995) (citing Blum v. Yaretsky, 457 U.S. 991, 1004-05 (1982)).

[60] *See* 962 F. Supp. at 1026.

[61] *See supra* note 1 and accompanying text.

[62] Electronic mail is analogous to courier services used by many businesses throughout the country. Courier services are provided by numerous private companies, none of which are governmental entities. For example, in Richmond, Virginia, a company could employ the services of Accurate Courier Express, B.E.X. Couriers Inc., Laser Courier, and Professional Courier Inc., to name a few. Accordingly, these courier services would have the right to restrict access to their property without violating the First Amendment because courier service is not an exclusive public function.

[63] Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp. 436, 442 (quoting Lloyd Corp. v. Tanner, 407 U.S. 551, 569 (1972)).

[64] *See id.*

[65] David J. Goldstone, *The Public Forum Doctrine in the Age of the Information Superhighway*, 46 Hastings L. J. 335, 353 (1995).

[66] *See* Mark v. Borough of Hatboro, 51 F.3d 1137, 1142 (3d Cir. 1995) (citing McKeesport Hosp. v. Accreditation Council for Graduate Medical Ed., 24 F.3d 519, 524 (3d Cir. 1994)).

[67] *See id.* (citing Burton v. Wilmington Parking Auth., 365 U.S. 715, 725 (1961)).

[68] *See America Online*, 948 F. Supp. at 445; CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997).

[69] Goldstone, *supra* note 66, at 356 (quoting Information Infrastructure Task Force, The National Information Infrastructure: Agenda for Action 5, 58 Fed. Reg. 49,025 (1993)).

[70] *Id.*

[71] *See America Online*, 948 F. Supp. at 444.

[72] *See id.* (quoting Tunstall v. Office of Judicial Support, 820 F.2d 631, 634 (3d Cir. 1987)).

[73] These two assumptions must be made before the freedom of speech clause of the First Amendment can be invoked. *See supra* note 43.

[74] *See* Rowan v. United States Post Office Dept., 397 U.S. 728, 737 (1970).

[75] *Id.* at 736.

[76] *See* CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1023 (S.D. Ohio 1997); America

Online's Complaint I, *supra* note 36; America Online's Complaint II, *see supra* note 36; Complaint at 4, Bigfoot Partners, L.P. v. Cyber Promotions, Inc. (S.D.N.Y. 1997) (visited Jan. 13, 1999) <http://www.jmls.edu/cyber/cases/bf-cp0.html> [hereinafter Bigfoot Complaint].

[77] *Rowan,* 397 U.S. at 736.

[78] "It would be an unwarranted infringement of property rights to require [CompuServe] to yield to the exercise of First Amendment under circumstances where adequate alternative avenues of communication exist." Cyber Promotions, Inc v. America Online, Inc., 948 F. Supp. 436, 443 (E.D. Pa. 1996) (quoting Lloyd Corp. v. Tanner, 407 U.S. 551, 567 (1972)).

[79] *See id*. at 443; *CompuServe Inc.,* 962 F. Supp. at 1026.

[80] *See, e.g., CompuServe Inc*., 962 F. Supp. at 1026-27; *America Online, Inc*., 948 F. Supp. at 445.

[81] For a brief discussion of the four-pronged Central Hudson/Fox test, see *supra* Part II (B).

[82] An argument could be made that the unsolicited email advertisements are misleading if the header information, the return address, or the domain name have been disguised by the sender.

[83] *See infra* Part V.

[84] Byars v. Bluff City News Co., Inc., 609 F.2d 843, 856 (6th Cir. 1980).

[85] *See generally* Restatement (Second) of Torts § 259 (1995).

[86] *See* Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp. 456, 464 (E.D. Pa. 1996).

[87] *See id*. at 456.

[88] *See id*.

[89] *See id*. at 462.

[90] *See id*.

[91] *See* A & B Refuse Disposers, Inc. v. Board of Ravenna Township Trustees, 596 N.E.2d 423, 425 (Ohio 1992).

[92] *See supra* notes 77-78.

[93] *See* CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1025 (S.D. Ohio 1997).

[94] *See id*.

[95] 962 F. Supp. 1015 (S.D. Ohio 1997).

[96] 948 F. Supp. 436 (E.D. Pa. 1996).

[97] No. CIV.A.97-5931, 1997 WL 634384 (E.D. Pa. Sept. 30, 1997).

[98] *See id*. at *1.

[99] *See id*. at *2, *4.

[100] *Id*. at *3.

[101] *See id*.

[102] 663 N.Y.S.2d 468 (Sup. Ct. 1997).

[103] *See id*.

[104] *See id*. at 470-71.

[105] *See id*. at 476.

[106] *See id*.

[107] Final Judgment, Parker v. C.N. Enterprises (D. Tex. 1997) (visited Jan. 20, 1999) <http://www.jmls.edu/cyber/cases/flowers3.html> [hereinafter Parker Final Judgment].

[108] *See id*.

[109] *See id*.

[110] *See id*.

[111] *See id*.

[112] *Id*.

[113] *See id*.

[114] *See, e.g.*, Bigfoot Complaint, *supra* note 77; Seidl Complaint, *supra* note 12; First Amended Complaint, Strong Capital Management, Inc. v. Smith (E.D. Wis. 1997) (No. 97-C-0371) (visited Jan. 14, 1999) <http://www.jmls.edu/cyber/cases/strong/comp1.html> [hereinafter Strong Capital Management]; Plaintiff's Original Petition and Application, Web Systems Corp. v. Cyber Promotions, Inc. (D. Tex. 1997) (No. 97-30156) (visited Jan. 14, 1999) <http://www.jmls.edu/cyber/cases/websys1.html> [hereinafter Web Systems].

[115] American Civil Liberties Union v. Reno, 929 F. Supp 824, 831 (E.D. Pa. 1996), *aff'd* 521 U.S. 844 (1997).

[116] *See* H.R. 4176, 105th Cong. (1998); H.R. 4124, 105th Cong. (1998); H.R. 1748, 105th Cong. (1998); H.R. 3888, 105th Cong. (1998); S. 1618, 105th Cong. (1998); S. 875, 105th Cong. (1997); S. 771, 105th Cong. (1997).

[117] Parker Final Judgment, *supra* note 108.

[118] *See id*.

[119] H.R. 4124.

[120] *See* S. 771.

[121] *See id*.

[122] Act of Aug. 27, 1998, 1998 Cal. Stat. 863. *See also* David Carney, *California Legislature Passes Anti-Spam Bill* (visited Jan. 14, 1999) <http://www.techlawjournal.com/internet/80831.htm>.

[123] *See* 1998 Cal. Stat. at 863.

[124] *See id*.

[125] To understand how a regulation can be drafted to increase a recipient's control, see *infra* part VII.

[126] *See* 1998 Cal. Stat. at 863.

[127] *See id*.

[128] *See* H.B. 2752, 55th Leg., Reg. Sess. (Wash. 1998).

[129] *See id*.

[130] *See id*.

[131] To understand how a regulation can be drafted to increase a recipient's control, *see infra* Part VII.

[132] H.B. 491, 20th Leg., Reg. Sess. (Alaska 1997).

[133] H.B. 337, Leg. Res. Comm'n, Reg. Sess. (Ky. 1998).

[134] H.B. 1114, 412th Gen. Assembly, Reg. Sess. (Md. 1998).

[135] H.B. 4581, 180th Gen. Ct., Reg. Sess. (Mass. 1997).

[136] H.B. 295, 208th Leg., Reg. Sess. (N.J. 1998); H.B. 513, 208th Leg., Reg. Sess. (N.J. 1998).

[137] S.B. 3524, 220th Leg., Annual Sess. (N.Y. 1997).

[138] H.B. 1744, 1997 Reg. Sess. (N.C. 1997).

[139] S.B. 1073, 1997 Reg. Sess. (R.I. 1997).

[140] H.B. 1325, 1998 Reg. Sess. (Va. 1998).

[141] S.B. 283, 1997 Reg. Sess. (Wis. 1997).

[142] *See supra* Part II. B.

[143] H.B. 1284, 61st Leg., Reg. Sess. (Colo. 1997).

[144] *See Unsolicited E-mail Statutes* (visited Jan. 14, 1999) <http://www.jmls.edu/cyber/statutes/email/state.html>.

[145] *See id*.

[146] *See id*.

[147] W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 14, at 85 (5th ed. 1984).

[148] *See* Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468, 472 (Cal. Ct. App. 1996); State v. Riley, 846 P.2d 1365, 1374 (Wash. 1993).

[149] *See e.g.* America Online's Complaint I, *supra* note 36; America Online's Complaint II, *supra* note 36; Complaint, Concentric Network Corp. v. Wallace (No. C-96-20829) (N.D. Cal. 1996) (visited Jan. 14, 1999) <http://www.jmls.edu/cyber/cases/concent1.html>; Complaint, Typhoon, Inc. v. Kentech Enters. (No. CV 97-6270 JSL) (S.D. Cal. 1997) (visited Jan. 14, 1999) <http://www.jmls.edu/cyber/cases/typhoon1.html> [hereinafter Typhoon Complaint]; Bigfoot Complaint, *supra* note 77; Plaintiff's Original Petition and Application, Parker v. C.N. Enterprises (No. 97-06273) (D. Tex. 1997) (visited Jan. 14, 1999) <http://www.jmls.edu/cyber/cases/flowers1.html>; Web Systems, *supra* note 115; Strong Capital Management, *supra* note 115.

[150] 962 F. Supp. 1015 (S.D. Ohio 1997).

[151] Parker Final Judgment, *supra* note 118.

[152] *See* 18 U.S.C. § 1030(a)(5)(A) (1994). *See, e.g.*, America Online's Complaint I, *supra* note 36; America Online's Complaint II, *supra* note 36; Concentric Complaint, *supra* note 150; Bigfoot Complaint, *supra* note 77; Strong Capital Management, *supra* note 115.

[153] 18 U.S.C. § 1030(a)(5)(A).

[154] *Id.*

[155] *Id.*

[156] *See id.*

[157] CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1028 (S.D. Ohio 1997).

[158] America Online's Complaint I, *supra* note 36.

[159] 15 U.S.C. § 1125(a)(1)(A).

[160] *See, e.g.*, America Online's Complaint I, *supra* note 36; America's Online Complaint II, *supra* note 36; Typhoon Complaint, *supra* note 150; Concentric Complaint, *supra* note 150; Juno Complaint, *supra* note 37; Bigfoot Complaint, *supra* note 77; Strong Capital Management, *supra* note 115.

[161] Typhoon Complaint, *supra* note 150.

[162] Janet Kornblum, *AOL Sues More Spammers* (visited Jan. 14, 1999) <http://www.news.com/News/Item/0,4,17872,00.html?>.

[163] American Library Ass'n v. Pataki, 969 F. Supp. 160, 169 (S.D.N.Y. 1997).

[164] *See* Courtney Macavinta, *Spam King, AOL Agree to Disagree* (visited Jan. 14, 1999) <http://www.news.com/News/Item/0,4,7648,00.html >.

[165] *See* Jerry Berman & Daniel J. Weitzner, *Abundance and User Control: Renewing the Democratic Heart of the First Amendment in the Age of Interactive Media*, 104 Yale L. J. 1619, 1621 (1995).

[166] *Id*. at 1632.

[167] *See* Carroll, *supra* note 8, at 270.

[168] *See* Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp. 456 (E.D. Pa. 1996).

[169] *See id*. at 457.

[170] *See* Macavinta, *supra* note 165.

[171] For a brief description of this blocking software, see *supra* notes 75-76.

[172] *See* Macavinta, *supra* note 165.

[173] *Id*.

[174] *Id*.

[175] *See* S. 771, 105th Cong. (1997) (pending in Senate).

[176] *See* Carroll, *supra* note 8, at 276.

[177] *See id*.

[178] Parker Final Judgment, *supra* note 108.

[179] 962 F. Supp. 1015 (S.D. Ohio 1997).
